International Journal of Engineering Research and General Science Volume 5, Issue 5, September-October, 2017
ISSN 2091-2730

Biometrics in Internet of Things (IoT) Security

R.Subha

Research Scholar, Department of Computer Science,

Mother Teresa Women's University, Kodaikanal

ABSTRACT*:* The "Internet of things" (IoT) is a hot topic of conversation both in the workplace and outside of it. Basically, IoT is a concept of connecting any device to the internet. This includes almost everything from mobile phone, washing machines, baby monitors, cars or even a jet engine of an airplane. IoT certainly opens the door to virtually endless opportunities but also to many challenges. Security vulnerabilities are big issues that are usually brought up in conversations. It's obvious that traditional approaches of user authentication are now inadequate and ineffective in the IoT era. This survey paper presents the security in the form Biometrics in Internet of Things security.

KEYWORDS: Internet of Things (IoT) , Interoperability , Privacy ,Security vulnerability, Internet

I. INTRODUCTION

The Internet of Things (IoT) is a dynamic global information network consisting of Internet-connected objects, such as Radio frequency identifications, sensors, actuators, as well as other instruments and smart appliances that are becoming an integral component of the future Internet. Over the last decade, we have seen a large number of the IoT solutions developed by start-ups, small and medium enterprises, large corporations, academic research institutes (such as universities), and private and public research organizations making their way into the market.

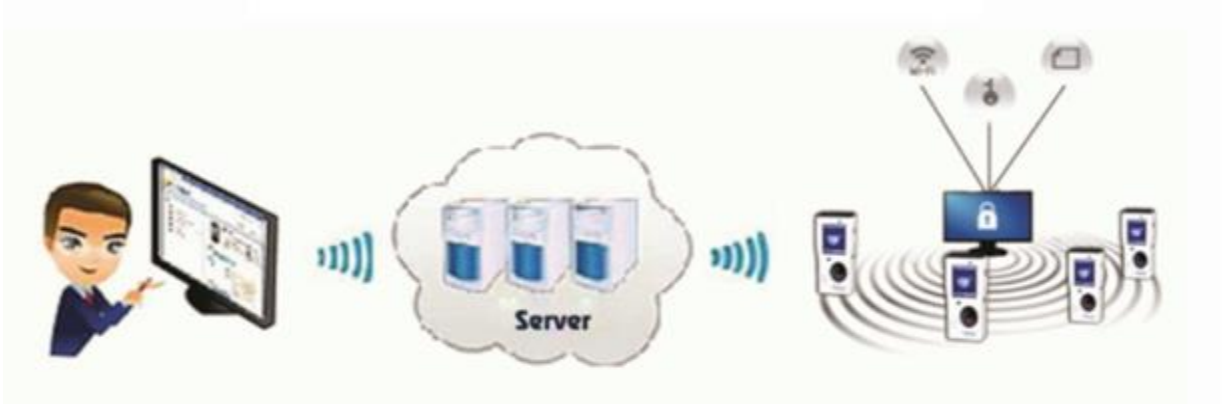

Fig 1.Iot Works in Biometrics

Biometric characteristics can be divided in two main classes, as represented in the following figure:

Physiological are related to the shape of the body. Examples include, but are not limited to fingerprint, face recognition, hand and palm geometry and iris recognition.

Behavioral are related to the behavior of a person. Characteristic implemented by using biometrics are signature verification, keystroke dynamics, and voice

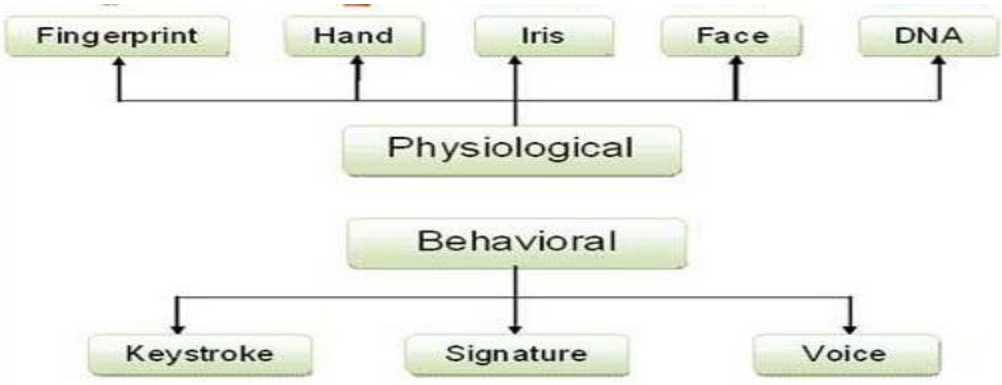

Fig 2. Types of Biometrics

A. *Finger print:* The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords – instead, only a touch provides instant access.

B. *Facial Image:* The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an optical camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. Major benefits of facial recognition are that it is non-intrusive, hands-free, and continuous and accepted by most users.

C. *Hand recognition:* These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand.

D. *Iris recognition:* This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification (1:1) and identification (1:N) modes (in systems performing one-to-many searches in a database). Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

E. *Retina Scan:* The human retina is a thin tissue composes d of neural cells that is located in the posterior portion of the eye. Because of the complex structure of the capillaries that supply the retina with blood, each person's retina is unique. The network of blood vessels in the retina is so complex that even identical twins do not share a similar pattern. Although retinal patterns may be altered in cases of diabetes, glaucoma, retinal degenerative disorders or cataracts, the retina typically remains unchanged from birth until death. Due to its unique and unchanging nature, the retina appears to be the most precise and

reliable biometric. Advocates of retinal scanning have concluded that it is so accurate that its error rate is estimated to be only one in a million.

F. *Signature recognition:* Biometric signature recognition systems will measure and analyze the physical activity of signing, such as the stroke order, the pressure applied and the speed. Some systems may also compare visual images of signatures, but the core of a signature biometric system is behavioral, i.e. how it is signed rather than visual, i.e. the image of the signature. Benefits of signature biometric systems: 1. While it is easy to copy the image of a signature, it is extremely difficult to mimic the behavior of signing; 2. Low False Acceptance Rates (FAR); 3. People are used to sign documents, so signature recognition systems are not perceived to be invasive.

G. *Voice or speech recognition:*

Voice or speech recognition is the ability of a machine or program to receive and interpret dictation, or to understand and carry out spoken commands. Strictly speaking, voice is also a physiological trait because every person has a different pitch, but voice recognition is mainly based on the study of the way a person speaks, commonly classified as behavioral.

II. THE INTERNET OF THINGS

With the growth of IoT and biometric technology, authentication is being completely re imagined. Deploying IoT security is one of the great challenges in the inter-connected world, and it requires a solution that relies on the strongest authentication.

This is the brave new world of the Internet of Things (IoT). The security vulnerabilities of the IoT are almost as varied as the devices and sensors connected to it.

Existing methods for authentication, such as passwords aided by a second factor, are being rendered moot due to human error as well as the enhanced sophistication of malware and other attacks.

III. THE BENEFITS OF BIOMETRICS

Biometric authentication is a conclusive, logical way to prove one's identity – a password can be replicated, for instance, but a fingerprint cannot.

Consumers are becoming more familiar with, and comfortable with, on-device biometrics. The latest Apple and Samsung mobile phones, as well as many new desktop and laptop computers, contain embedded biometric sensors.

When authenticating to a smart lock, or even a smart car it is important that authentication take place on the smart device rather than on the user's end. Malware may be used to spoof the authenticated user identity and unlock a smart node without the proper credentials.

Authentication is essentially split across both the user's mobile device and the lock itself when validation capability is embedded directly into a smart lock. A secure lock becomes a standalone biometric validation server, and cannot be remotely authenticated without the presence of a trusted biometric device.

Mobile devices with embedded biometric sensors are changing how users authenticate to services they use every day, including email, social media, banking – and now for physical access.

The IoT is a revolution in how we communicate and interact with the world around us. It is a growing entity with almost as many security pitfalls as work and life advantages. There are many more devices to potentially be hacked, and when it comes to securing intellectual property and mission-critical applications, enterprises, financial institutions and government agencies cannot take chances.

Older forms of user authentication simply cannot combat today's advanced and sophisticated security threats. Advances in biometric technology have enabled this method of authentication to be embedded in the mobile devices we use every day. It's a scalable security solution that can help organisations of all types and sizes stay ahead of the cyber criminals

Listed below is everything that one needs to know about biometric systems and Internet Of Things (IOT) as the essential factor:

IV. PURPOSE

- ✓ Basically designed to ensure secure identification purposes with highly optimized usage of existing technologies and resources.
- ✓ Create no-password criteria in the various interfaces dealing with confidential authentication systems.
- ✓ Inculcate decentralization of the biometric systems and provide greater encryption standards.

V. APPLICATIONS

Biometric attendance system, security and encryption standards are duly incorporated into various fields for application on a greater scale. What stands to create the perfect rendering of these "secure systems" is the highly revolutionized "Internet of Things" technology that facilitates better assurance of deployment for maximum security standards.

A. *Banking and E-Payment:* Payment solutions through online or mobile mode, Block chain Systems, E-Trading facilities, and the like.

B. *Corporate and Enterprise levels:* Facilitate authorized Employee Access (direct or remote).

C. *Individual User Level:* IoT features in smart solutions for homes, cars, and other personal belongings, etc.

D. *Health Care Organizations:* Easy retrieval and monitoring of the corresponding user data for better analysis of health statistics.

VI. FEATURES

- ✓ Complete authentication with full time security feature.
- ✓ High end monitoring of the secured systems on the go.
- ✓ Full time support systems to deal with any kind of issues generated during the corresponding operation.
- ✓ Smart and creative user interface to facilitate enhanced user experience
- ✓ Personalization features specifically in terms of the desired requirements
- ✓ Affordable smart security solutions and totally worth the investment.
- ✓ Detailed report generation and analysis of the obtained data for further varied purposes.
- ✓ Real time execution of the biometric data obtained for authorization of various related procedures.
- ✓ Quicker and faster solutions with improved efficiency.
- ✓ Highly improved alert features with necessary strategic steps for the same.
- ✓ Greater security standards through complex encryption algorithms and n-step authentication procedures for best applicability on a universal scale.
- ✓ Complete digitization of data for better integration into other applications.
- ✓ Multi layer security levels for better hack-proof solutions.
- ✓ Cross platform synchronization features

VII. ADVANTAGES

- ✓ Go Password-less with the implementation of IoT based biometric security systems. No more requirements to type in cumbersome passwords or remember one as such.
- ✓ Better proofing against existing security breaches through multi layer security levels.
- ✓ On the go monitoring facility helps implement and improvise security solutions as per the need of the hour.
- ✓ Compatibility to various platforms and devices creates much favorable response from the client end
- ✓ Personalized biometric security features help create different security standards for different purposes.
- ✓ Greater ease of validation of biometric data obtained.
- ✓ One stop solution for all requirements -the same biometric information can be used for other security applications too.
- ✓ Modular segregation of the biometric system from the core operations, to differentiate malware from creating potential risks to the mainstream functionalities.
- ✓ Authentication done at the smart device. Modularity of the same between the user's mobile and the smart device provides for greater decentralization of security factors.
- ✓ IoT based biometric systems can also be used for authenticating individual presence. Hence, a more efficient way to prove an individual's location record.
- ✓ Full time support assistance creates better implementation feasibility.
- ✓ Mapping of biometric data is literally tough to replicate, hence more popular than traditional passwords.
- ✓ Reduces time complexity to a fairly large extent.

VIII. DISADVANTAGES

- ✓ A single failure in a particular module can create a chain reaction of deactivation, if proper modularity is not ensured.
- ✓ Improper functioning of the authenticating device or software corruption can pose open path for security breaches.
- ✓ Inadequate knowledge of the functioning of IoT based biometric systems can cause potential risk for essential data.
- ✓ IoT technology has undoubtedly become a part and parcel of the existing lifestyle and is in fact taken things to a digital level with every step in the positive direction. When considered from a user point of view, simple facilitation of security systems via IoT has effectively lowered the potential to possible threats. Also with greater manageability options on their very own specific devices and customized authentication procedures for the same, things from basic to highly confidential status can easily be monitored closely for enhanced security standards via the IoT technology.

IX. CONCLUSION

Biometrics in IoT will not only unlock bank apps, email accounts but also cars, homes and many other things. "We conservatively estimate that biometric sensors, which includes work time management and premise security entry consoles, will total at least 500 million "Internet of Things" connections by the upcoming years." With the evolution of the IoT and the utilizing of biometrics, there will be endless applications giving both convenience and security in different industries such as: smart home, automotive industry, finance, healthcare, etc. which will only be limited by human's imagination.

REFERENCES:

1.http://www.iritech.com/blog/internet-of-things-1016
2.”THE BIO-T: THE BIOMETRIC INTERNET OF THINGS” GEORGE AVETISOV, CEO AND CO-FOUNDER, HYPR CORP. NOVEMBER 11, 2016
3. “Biometrics to Secure the Internet of Things”, https://www.engadget.com/2015/10/08/biometrics-to-secure-the-internet-of-things.
4.” The Internet of things”, Gershenfeld N, Krikorian R, Cohen D (2004). Sci Am 291(4):76–81
5. “Biometrics in Internet of Things (IoT) security” Published on September 26, 2016 Narsimhmaswamy badugu, https://www.linkedin.com
6. G. Santucci. From Internet to Data to Internet of Things. Proceedings of the International Conference on Future Trends of the Internet. (2009).
7. “The Internet of Things: A Survey” L. Atzori, A. Lera, and G. Morabito, 2787-2805. (2010). 3. Lutz Heuser, Zoltan Nochta, Nina-Cathrin Trunk. ICT Shaping the World: A Scientific View. ETSI, WILEY Publication.(2008).
8. Internet of Things - Applications and Challenges in Technology and Standardization”, Debasis Bandyopadhyay · Jaydip Sen, Wireless Personal Communications manuscript.
9. “Internet of Things”,Feng Xia, Laurence T.Yang, Lizhe Wang and Alexey Vinel, ,INTERNATIONAL JOURNAL OF COMMUNICATION SYSTEMS, Volume 25, Issue 9, pages 1101-1102, September 2012 12.
10.“That ‘Internet of Things’ Thing”, Kevin Ashton, RFID journal, June 2009, http://www.rfidjournal.com/articles/view?4986